

SITE SECURITY REVIEW WORKSHEET

NOTE: National Change Of Address Linkage System (NCOA^{Link}) is a USPS® (United States Postal Service) sensitive information resource which will be housed in the facilities of potential NCOA^{Link} Licensed Service Providers (Licensees) following approval of all documentation, testing and certification. This USPS Security Document has been adapted for companies seeking Licenses for USPS sensitive information.

USPS Site Information Security Review Worksheet Instructions	
Purpose	The <i>Site Information Security Review Worksheet</i> has been designed to determine the level of risk associated with a facility housing USPS information resources. It equips decision makers with the facts they need to make informed decisions to manage risk at acceptable levels using cost-effective security controls.
Site Security Review Areas	<p>The Site Security Review assesses physical security controls that could affect the availability, confidentiality and integrity of USPS information resources. The review evaluation risks in the following areas as they relate to the physical security of information resources:</p> <ol style="list-style-type: none"> 1. Site Location. 2. Facility Physical Security. 3. Controlled Area Physical Security. 4. Equipment and Media Controls. 5. Environmental Controls. 6. Communications Controls. 7. Personnel Security. 8. Auditing and Monitoring. 9. Emergency Response and Business Continuity.
Who completes the worksheet	The Site Security Review is completed by the Facility Manager with the assistance of the Information Systems Security Officer (ISSO), site Security personnel, and/or the equivalent at the potential Licensee site.
What information resources need a Risk Assessment	USPS information resources classified as business-controlled, critical, or sensitive are required to have completed a Site Security Review for all facilities where components of the information resource will be developed or housed for production. Facilities that have undergone a Site Security Review in the past three years may submit the previous Site Security Review Worksheet for consideration if no changes have been made to the site's security.
When to complete the worksheet	The worksheet must be completed during the Documentation phase (Step 1) of the NCOA ^{Link} Licensing process.
How to complete the worksheet	The worksheet has been designed to provide an easy to use tool to assess risk. When completing the worksheet you will be asked to fill in a check box. In several sections you will be asked to provide a response comprised of several words. An electronic copy of the worksheet may be obtained from the RIBBS website at http://ribbs.usps.gov/files/NCOALink .
Completed worksheets	Upon completion the worksheet must be submitted to the USPS National Customer Support Center for approval.

USPS Site Security Review	Site <input style="width: 150px;" type="text"/>								
Section 1: Site Overview									
A. Identify location of the site and facility	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 150px; border: none;">Facility</td> <td style="border: 1px solid black; height: 30px;"></td> </tr> <tr> <td style="border: none;">Location</td> <td style="border: 1px solid black; height: 30px;"></td> </tr> <tr> <td style="border: none;">Facility Manager</td> <td style="border: 1px solid black; height: 30px;"></td> </tr> <tr> <td style="border: none;">Facility Manager Telephone #</td> <td style="border: 1px solid black; height: 30px;"></td> </tr> </table>	Facility		Location		Facility Manager		Facility Manager Telephone #	
Facility									
Location									
Facility Manager									
Facility Manager Telephone #									

Section 2: Site Security Checkpoints			
<p>To determine risks based on the geographic locations of a site, initial research should be conducted to determine the threats present in the area. Statistical data on natural disasters by location can be obtained at the Federal Emergency Management Agency (FEMA) sponsored website: http://www.esri.com/hazards/</p> <p><i>Please evaluate the following physical security controls by checking the most appropriate box.</i></p>			
	YES	NO	Not Applicable
A. Site Location Physical Security			
a) If the site is located in an area of high seismic activity, are appropriate controls in place to protect the facility and information resources contained within?			
b) If the site is located in a 100-year flood plain, have flood controls been implemented to protect the facility and information resources (computer room above the 2 nd floor, flood insurance)?			
c) If the site is located in an area with high potential for fire hazards (wild-fires, dry grasslands or forest areas) have appropriate fire controls been implemented?			
d) If the building is in a hurricane or tornado zone have the appropriate controls been implemented?			
e) If the site of the facility is located near an airport, interstate highway, railroad or industry that poses a threat to the facility, have controls been implemented to adequately protect the facility?			
f) Is the facility located in an area of high crime? (Check with local law enforcement agency for statistical information)			
g) If the facility shares common walls or doors with a neighboring business, is access controlled?			
h) Other site location concerns: (please list)			

B. Facility Physical Security		YES	NO	Not Applicable
a)	Is there a facility security officer assigned to the building?			
b)	Is the perimeter of the site protected by physical barriers (fences)?			
c)	Is exterior and interior lighting adequate to detect and deter unauthorized activities?			
d)	Have all entry points been identified?			
e)	Are physical access controls in place at all entry points for personnel and equipment?			
f)	Are all entrances locked or secured with an access control system?			
g)	Are specialist personnel employed to control access of personnel and equipment at key entry points?			
h)	Is there one primary equipment and materials entry point?			
i)	Is there surveillance equipment at entry points?			
j)	Is the facility alarmed and or using a licensed and bonded 24-hour monitoring service, patrol, or inspection?			
k)	Is physical access controlled by a computerized system?			
l)	Can access be controlled manually in an event of a failure of the physical access control system?			
m)	Are there lock status sensors on all entry points?			
n)	Is badge entry employed at entry points for personnel?			
o)	Do all personnel wear their badges externally, and is this enforced?			
p)	Are pictures required on badges for all personnel?			
q)	Is there a procedure for replacement of lost or forgotten badges?			
r)	Are all visitors required to sign-in and out?			
s)	Are visitors escorted by personnel at all times while within the facility?			
t)	Is there a procedure in place to ensure key management and accountability (key checkout, return of keys, termination of employment, etc.)?			
u)	Is a list of those holding badges or keys maintained and reviewed periodically?			
v)	Are lock combinations changed frequently, or when personnel who know the combination terminate or change employment?			
w)	Are restricted areas identified within the facility?			
x)	Are uninterruptible power supplies (UPS) used for all physical access control devices (readers, door strikes, motion detectors, etc.)?			
y)	Are cameras, computerized security system, and/or surveillance equipment in working order?			
z)	Are videotapes maintained for at least 30 days and replaced annually?			
aa)	Other facility physical security concerns: (please list)			

C. Controlled Area Physical Security (data centers, server rooms, switch facilities, telephone or wiring closet, media storage areas)			
	YES	NO	Not Applicable
a) Are all critical or sensitive information resources located within controlled areas?			
b) Have critical and sensitive information resources been segregated from non-sensitive and non-critical systems?			
c) Is there low visibility (no unnecessary signs) for each controlled room?			
d) Is access to controlled areas restricted to only personnel with a need to know?			
e) Is an access roster maintained and reviewed for each controlled area?			
f) Does the controlled area have full-height walls and fireproof ceilings?			
g) Does the controlled area have two or fewer entrance points?			
h) Are the doors to the controlled area solid, fireproof, lockable and observable by security staff?			
i) Are windows small, lockable, or barred?			
j) Are flammable material prohibited from directly below or within controlled areas?			
k) Have temporary security procedures been placed in effect for any controlled area currently under construction?			
l) Other controlled area physical security concerns: (please list)			

D. Equipment and Media Controls Security			
	YES	NO	Not Applicable
a) Is an inventory of equipment maintained in a secure location?			
b) Is equipment marked in an obvious, permanent and easily identifiable manner?			
c) Is equipment located within controlled areas placed where it cannot be seen or reached from a door or a window and away from radiators, heating vents, air conditioning, or other ducts?			
d) Are critical and sensitive information resources located in lockable cabinets (racks) when possible to prevent unauthorized tampering?			
e) Is check-out and check-in required when removing or bringing in equipment from the facility?			
f) Is off-site repair or maintenance of equipment preauthorized, and all equipment being taken off-site sanitized of restricted information prior to maintenance?			
g) Are portable devices (laptops, hand held devices, etc.) secured when unattended and files containing restricted information encrypted when appropriate?			
h) Are photocopiers, fax machines, printers and scanners located in public view so usage can be monitored?			
i) If hardcopy output is held in a restricted area, is a log maintained for all deliveries and pickups?			

j) Do workstations employ screen savers or screen locking when unattended?				
k) Is media containing restricted information disposed of in a manner that prevents recovery?				
l) Is backup media stored in a controlled area?				
m) Have qualified technicians been identified to repair critical equipment when it fails? Is their contact information stored in a secure and accessible location?				
n) Are deposits and withdrawals of tapes and other storage media authorized and logged?				
o) Other equipment and media control concerns: (please list)				

E. Environmental Controls Security

	YES	NO	Not Applicable
a) Are environmental controls stored in a secure area and centrally monitored and alarmed to notify staff when environmental conditions move outside of predetermined ranges?			
b) Are eating, drinking and smoking prohibitions in information resource areas regulated and enforced?			
c) Is all non-essential flammable waste removed from the building?			
d) Is adequate fire detection, suppression, and notification equipment properly maintained and routinely tested?			
e) Does the fire alarm sound at an internal security station or guard post or centralized building location?			
f) Are possible fire ignition sources such as failures of electronic devices or wiring, or improper storage devices reviewed periodically?			
g) Are rooms with information resources kept at reasonable temperatures? (60-70° F)			
h) Are there redundant power feeds or backup power generators for the facility?			
i) Are there backup power generators for environmental services and are they tested periodically?			
j) Are rooms with information resources kept at acceptable humidity levels (20-70 percent)?			
k) Is there a redundant cooling system or tower to protect against the failure of the primary system?			
l) Are drains cleaned regularly?			
m) Are the locations of building plumbing lines known and are they located such that they do not endanger systems?			
n) Are water detectors installed on the floor near computer equipment?			
o) Are liquid proof covers kept near computer equipment?			
p) Do computer rooms have raised flooring?			
q) Are uninterrupt power supplies (UPS) used on all critical equipment?			
r) Are line filters installed to control voltage spikes to minimize damage from power fluctuations?			

s) Is there battery operated lighting throughout the building in case of a power outage?				
t) Other environmental control concerns? (please list)				

F Communications Physical Security	YES	NO	Not Applicable
a) Are communications circuits routed to avoid single points of failure?			
b) Are communication device backups (routers, gateways, switches) kept on site?			
c) Are primary and alternate communication circuits documented?			
d) Is preventative maintenance conducted on all communication devices?			
e) Are communication cables protected (concealed installation, secure conduit, alarmed, termination points, route restrictions)?			
f) Is physical access to data transmission lines controlled?			
g) Is hardware failure monitoring/fault isolation conducted?			
h) Are in-house telephone exchanges and associated equipment and cabling in a controlled area?			
i) Are communications facilities critical to the continuity of network services identified and have arrangements been made to enable services to be resumed promptly?			
j) Are voice, video, faxes, and in-house telephone exchanges configured to support peak loads?			
k) Are maintenance contracts in place to assure timely repair of communications equipment?			
l) Are tamper switches installed on critical or sensitive hardware?			
m) Are equipment and media inventories maintained?			
n) Are locking racks used for sensitive communications media and hardware?			
o) Is perimeter security in place to protect the internal Postal Service network?			
p) Other communications physical security concerns: (please list)			

G Personnel Security	YES	NO	Not Applicable
a) Are appropriate security clearance obtained for personnel?			
b) Are appropriate clearances or background screenings verified prior to allowing personnel access to controlled areas?			
c) Are new personnel required to sign a non-disclosure agreement?			
d) Do personnel receive training regarding security policy or security awareness?			
e) Do personnel receive training in physical security and emergency procedures?			
f) Does management regularly review who has access to controlled areas?			

g) Do personnel receive training on employee vigilance/surveillance (questioning unrecognized individuals, watching for suspicious activity)?			
h) Are termination procedures in place to immediately terminate existing physical access when an individual terminates employment or transfers to another position?			
i) Are termination procedures followed?			
j) Is security staff provided with an up-to-date list of all personnel access privileges?			
k) Are periodic reviews of access lists compared to current personnel and contract files?			
l) Are maintenance personnel (technical vendors) monitored while accessing controlled areas?			
m) Do cleaning personnel have their own keys to controlled areas (to establish individual accountability)?			
n) Are cleaning personnel monitored while in controlled areas?			
o) Other personnel security concerns: (please list)			

HAuditing and Monitoring Security

	YES	NO	Not Applicable
a) Are physical security problems and incidents documented?			
b) Are physical inspections of the site, facility, and controlled areas conducted on a regular basis both during normal business hours and after hours?			
c) Are auditing and monitoring procedures and controls in place and accountability for reviewing logs assigned and scheduled?			
d) Is an approved banner appropriately displayed?			
e) Are computer users assigned a unique user ID?			
f) Are users required to authenticate to information resources?			
g) Are passwords one-way encrypted?			
h) Does access control force the frequent changing of passwords?			
i) Is user ID terminated after six failed access attempts?			
j) Is logging enabled at the application and network level?			
k) Are security logs kept for invalid password attempts and file access and reviewed periodically?			
l) Are audit logs maintained for a time period appropriate to the information resource and sufficient for evidentiary purposes?			
m) Is restricted information encrypted while stored on an information resource and backup media?			

n) Are controls in place to restrict access to Postal Service information resources?				
o) Other auditing and monitoring concerns: (please list)				

I. Emergency Response and Business Continuity

	YES	NO	Not Applicable
a) Are emergency response procedures documented and tested?			
b) Are fire drills and fire-safety inspections periodically conducted?			
c) Are evacuation routes away from the site identified?			
d) Are adequate procedures in place to inform personnel of impending emergencies?			
e) Is there an emergency notification call-tree developed, maintained and distributed so that critical staff can be notified during an emergency?			
f) Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills or other emergencies?			
g) Have Disaster Recovery plans been developed in accordance with established policies, guidelines and templates?			
h) Is Disaster Recovery plan stored in a secure location and retrievable if the facility is inaccessible?			
i) Are Disaster Recovery plans tested and the results reviewed according to established policy?			
j) Are critical backups stored off-site?			
k) Other emergency response and business continuity concerns: (please list)			

Section 3: Site Security Evaluation

Physical security controls that have not been implemented may pose a significant risk to the information resources housed at a facility. In this section please document all security controls in sections 2-9 that were marked as "NO." Controls that have not been implemented should be analyzed to determine the risk level not implementing the control would pose to the facility and information resources housed therein.

Risk Metrics

The risk levels for the Site Security Review have been assigned the following metric descriptors of high, moderate, low and none.

Step 1: Analyze Probability and Impact to Determine Risk

The following metrics are used in this process to determine the overall risk:

- 1) Likelihood of Occurrence
 - a) High Likelihood: frequent; likelihood of repeated incidents.
 - b) Moderate Likelihood: occasional; likelihood of incidents sometime in the next year.
 - c) Low Likelihood: slight; incident may infrequently or rarely occur.
 - d) No Likelihood: improbable; incident not likely or practically impossible to occur; or not applicable to the information resource.
- 2) Impact to the unavailability, modification, disclosure, or destruction of information resources.
 - a) High Impact: significant compromise or disruption of mission or possible injury to personnel.
 - b) Moderate Impact: transitory disruption to the mission but not injury to personnel.
 - c) Low Impact: negligible impact to mission, but no injury to personnel.
 - d) No Impact: no measurable impact to mission, and no injury to personnel.

Step 2: Determine the Overall Risk Level

After determining both the likelihood and impact, use the Overall Risk Determination Table below to determine the overall risk rating posed by that unimplemented control.

On the following page, for each unimplemented control please check a box to indicate the overall risk level.

	High Impact	Moderate Impact	Low Impact	No Impact
High Likelihood	HIGH RISK	HIGH RISK	MODERATE RISK	NO RISK
Moderate Likelihood	HIGH RISK	MODERATE RISK	LOW RISK	NO RISK
Low Likelihood	MODERATE RISK	LOW RISK	LOW RISK	NO RISK
No Likelihood	NO RISK	NO RISK	NO RISK	NO RISK

Section 4: Site Security Review Summary

This section documents the overall risk status of the facility; please document all high to moderate risks identified in section 3 and the plan for how the risk will be managed.

High Risks:

Please document high risks identified, and how these risks will be mitigated. High risks must be mitigated.

Moderate Risks:

Please document all moderate risks identified for the site, and a plan for how these risks will be mitigated. A plan for mitigating the risk must be documented for all moderate site risks.

Section 5: Completion details

1. Site Security Review Completed By:

a) Name

--

b) Signature

--

c) Contact Information

--

2. Facility Manager Signature:

--

3. Site Security Review Date:

Day	Month	Year
<input type="text"/>	<input type="text"/>	<input type="text"/>